RSAC 2025 Conference

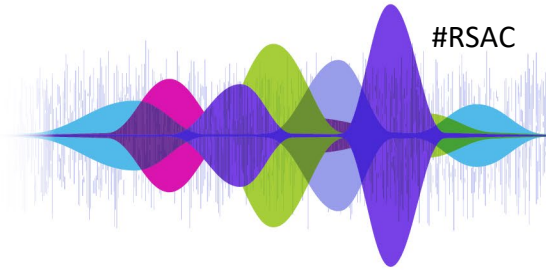
Many Voices.
One Community.

SESSION ID: GRC-W08

Navigating Cyber Risk Insurance—Pre and Post "Boom"

Sarah W. Anderson

Owner & Founder
SWA Law LLC & LegallyCyber.com
https://www.linkedin.com/in/swa-legallycyber/



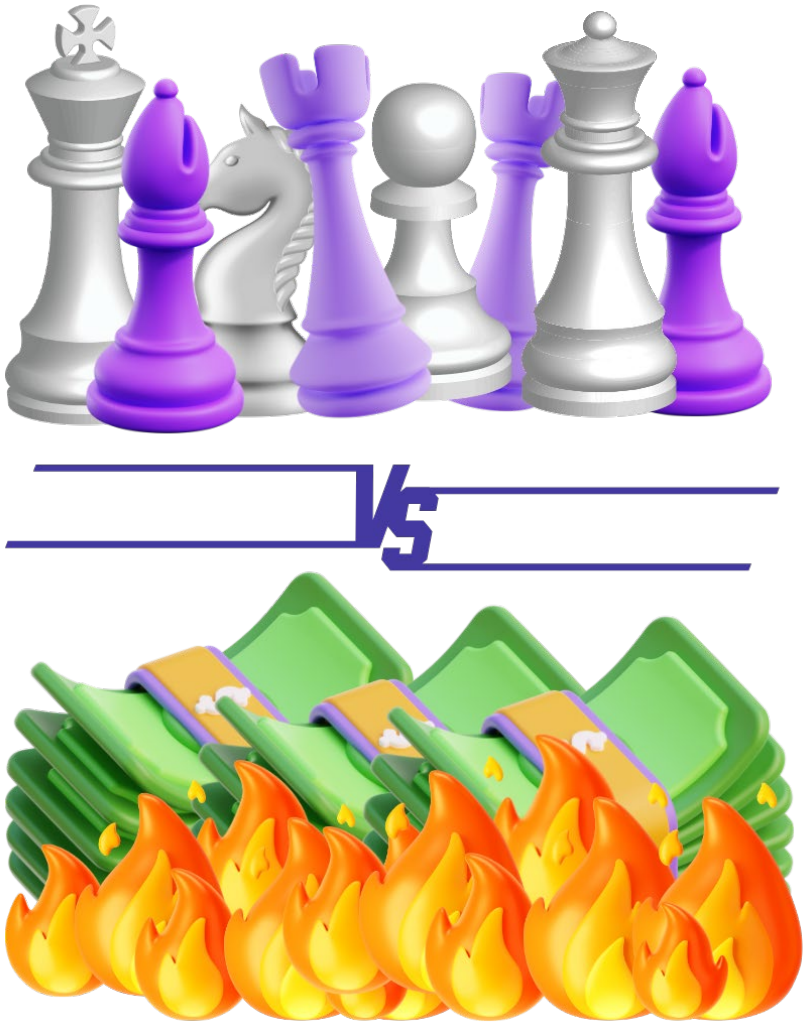
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

THEME



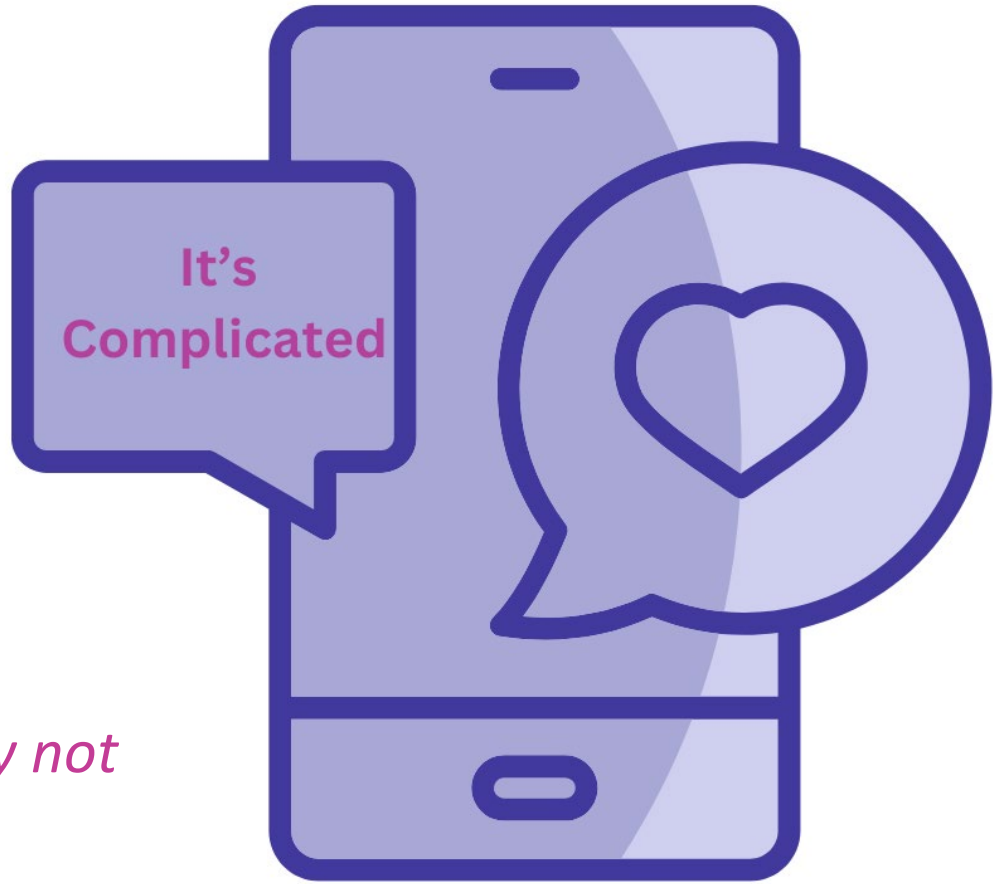
www.giphy.com

COMPETING MOTIVATIONS

1. Cyber Insurance is unlike traditional insurance – failure to buy a policy that accurately reflects your entity's needs wastes money.

2. Cyber Insurance is ***absolutely needed*** for financial readiness.

3. **BUT**, the insurer's goals are not aligned with those it insures.



*Psst…and the insurer's vendors **may** (but certainly not all) also have conflicting goals…*

A LITTLE...

IMMATURE MARKET

- **1997:** AIG writes first cyber policy on internet security. No data existed to measure risks and price policies – very small market.

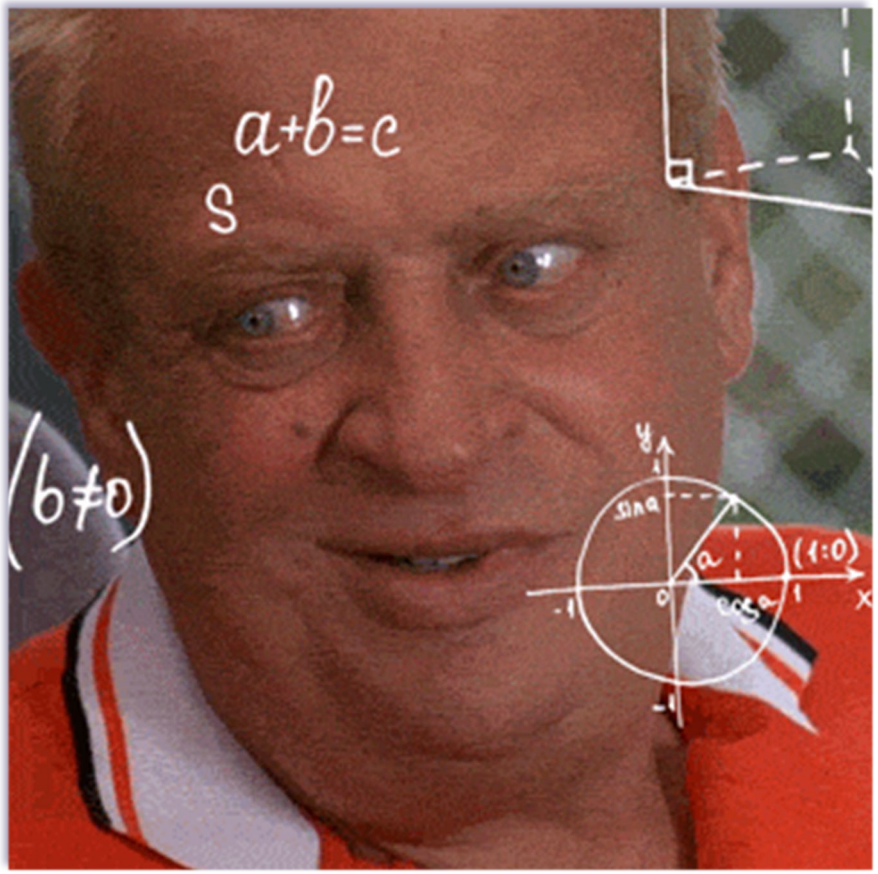
- **Early & Mid-2000s:** Cyber insurers offer 1st party coverage.
  - Profit margins small and policies unpopular
  - **2003-2008**: 34 states breach reporting laws.

- **2010s:** Equifax (2017), Target (2013), BlueCross (2015), Marriott (2016).

- **2017:** Cyber is fastest-growing insurance market. More than $3 Billion in premiums.

- **2020**: Covid hits, everyone telecommutes, and cyber-attacks rise more than 300%.

ACTUARIAL CONFUSION

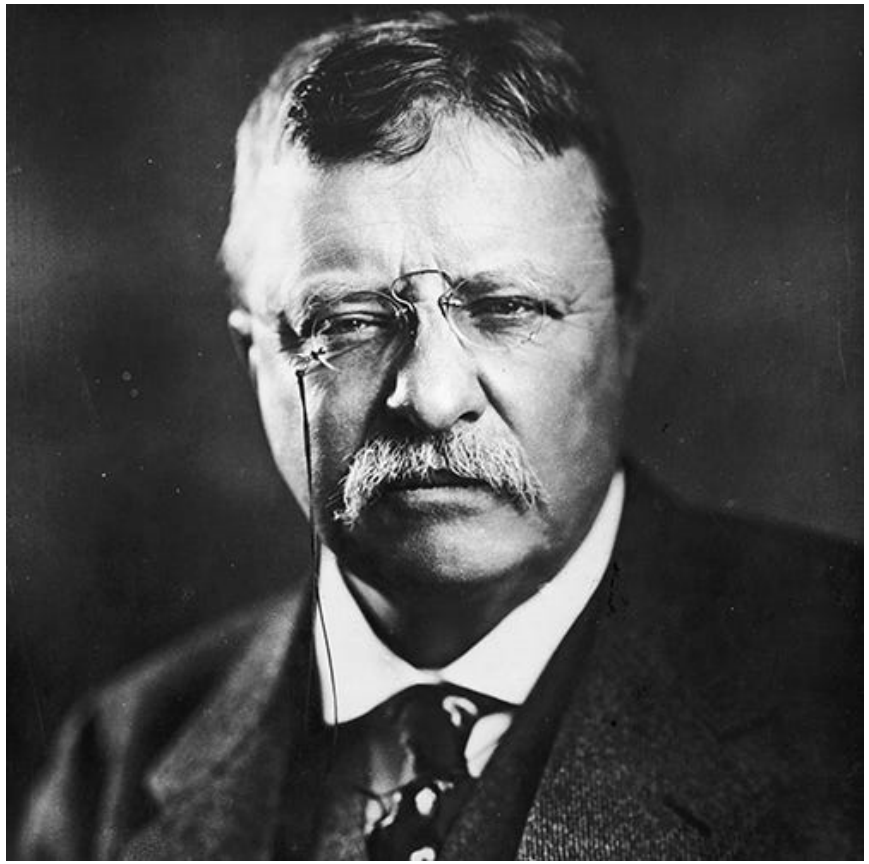


www.giphy.com

The earliest computer viruses are from the 1980s. Insurers lack decades of claims data to inform actuarial models used to predict risks and payouts. Cyber risk was/is indeterminable, able to impact an endless number of insureds at any time.

With auto and home-owners insurance, it is extremely unlikely that millions of insureds across the nation would experience huge unquantifiable losses simultaneously. **The same is not true for cyber losses.**

APPROACH



“Complaining about a problem without posing a solution is called whining.”

Theodore Roosevelt

PRE-BOOM

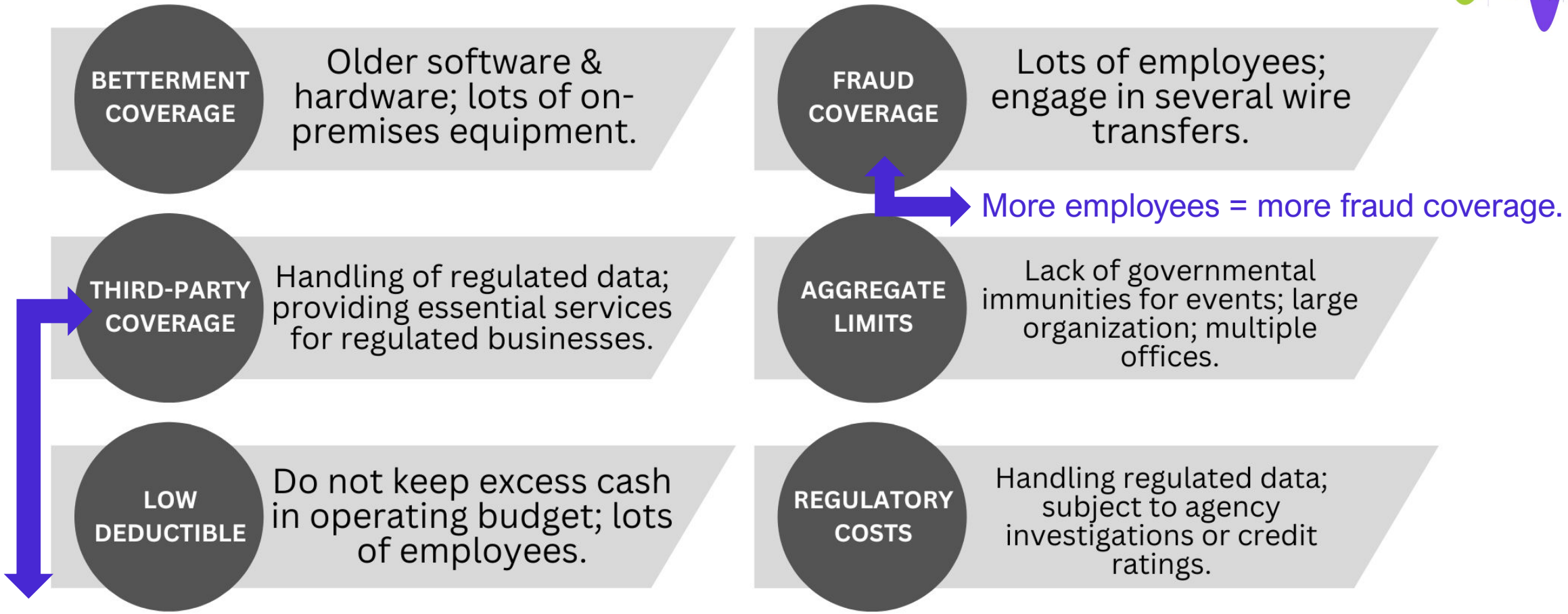
Study the chess board. Put yourself in the best position before a cyber-attack and insurance claim.

SHOPPING FOR CYBER INSURANCE

Cyber policies are “Cafeteria Style.” Before buying insured must evaluate:

- Age of current software and hardware.
- Cloud-based or on-premises servers.
- Third-parties with network privileges.
- Number of users.
- Handling of any regulated data:
  - Biometrics / Healthcare
  - Banking / Minor Children
- Ability to pay deductibles.
- Engaging in any wiring of funds.
- Cost of downtime (after a cyber incident)
- Potential need to add additional insured(s).

IDENTIFYING YOUR NEEDS


BETTERMENT COVERAGE
Older software & hardware; lots of on-premises equipment.
FRAUD COVERAGE
Lots of employees; engage in several wire transfers.
More employees = more fraud coverage.
THIRD-PARTY COVERAGE
Handling of regulated data; providing essential services for regulated businesses.
AGGREGATE LIMITS
Lack of governmental immunities for events; large organization; multiple offices.
LOW DEDUCTIBLE
Do not keep excess cash in operating budget; lots of employees.
REGULATORY COSTS
Handling regulated data; subject to agency investigations or credit ratings.

First-party coverage is standard. Third-party coverage protects from lawsuits and claims by those impacted by insured's incident.

IDENTIFYING YOUR NEEDS

More employees **EQUALS** more people susceptible to fraud and social engineering.

BUT: Computer Fraud **DOES NOT EQUAL** Social Engineering.

Social Engineering has ***intentionally*** **lower** default coverage. Fraud has **higher** default coverage, but harder to satisfy.

IDENTIFYING YOUR NEEDS

TRAVELERS

Social Engineering Fraud.

Means intentionally misleading an *Insured Person*, by providing an instruction that:

1. is not made by an *Insured*;
2. is purportedly from a *Vendor*, *Client*, or *Insured Person*;
3. directs the *Insured Person* to transfer, pay, or deliver *Money* or *Securities*;
4. contains a misrepresentation of material fact; and
5. is relied upon by the *Insured Person*, believing the material fact to be true.

$100K Max Coverage
$5K Deductible

Computer Fraud.

1. Means an intentional, unauthorized, and fraudulent entry or change of data or computer instructions, directly into or within, a *Computer System*, that:
   a. is not made by an *Insured Person*, an *Independent Contractor*, or any other person under the direct supervision of the *Insured*; and
   b. causes *Money*, *Securities*, or *Other Property* to be transferred, paid, or delivered from inside the *Insured Entity's* premises or the *Insured Entity's* financial institution premises to a place outside of such premises.
2. Does not include *Social Engineering Fraud*.

$250K Max Coverage
$5K Deductible

IDENTIFYING YOUR NEEDS

- Betterment coverage sometimes available.
- Without it, insurer *potentially* reimburses for lost/destroyed equipment at its value ***at the time of the incident***.
- Seeking ins. coverage with dated networking equipment/software invites cyber-attacks and minimizes any insurance benefit.
- Better to invest in network before seeking coverage
- Reduces premiums, helps prevent incidents, and elicits higher ROI following incident.

IDENTIFYING YOUR NEEDS

- Regulated data (healthcare, finance, biometrics/genetics, data belonging to minors, data brokers) requires more third-party and legal coverage.
- More likely to:
  - Get sued by private citizens.
  - Requires defense in regulatory investigations.
  - At greater risk of third-party damages through vendor/partner agreements.
- Examine the “downstream effects.”

APPLYING FOR COVERAGE

Are you aware of a situation or circumstance which could result in a claim against you with regard to issues related to the cyber coverage you are seeking? ☐ Yes ☐ No

a. If yes, please describe:

- Prepare to answer 20+ questions about the network. Do **NOT** lie.
- Insurer's questionnaires are intentionally "nitpicky."
- If unsure, give the most conservative answer. Policy are invalidated for falsities.
  - **BE HONEST, NOT ASPERATIONAL.**
- Questions that begin with "are ***you*** aware" are not asking the employee but the ***entity itself,*** including anyone employed there.
  - NO comfort in lack of knowledge – ask someone!

HORROR STORY

Travelers v. International Control Services, Inc.,
(C.D. Ill. July 6, 2022)

- **Background:** International Control Services (ICS), an electronics manufacturer suffered ransomware event. Sought coverage via its Travelers cyber policy.

- **Issue**: ICS' cyber application stated all servers "**required**" MFA.
  - But the compromised server had MFA enabled ***not enforced***.

- **Resolution**: Travelers and ICS agreed to stipulate that Travelers relied upon incorrect statements in ICS application. Policy declared voidfrom inception.

- **Takeaway:** Failing to perform any security req. may rescind policy.
  - All it takes is one employee to say "What Requirement?"

POST-BOOM

Play to Win - Understanding the rules of the game and players' motivations.

PLAYER EXPECTATIONS

INSURER

- Timely claim submission (30 days, before end of coverage period).
- Communication with the adjuster.
- Cooperate with the panel vendors or justify use of other vendors.
- Seek approval before incurring reimbursable expenses.
- Discuss regulatory reporting before executing.
- Mitigate losses as much as possible

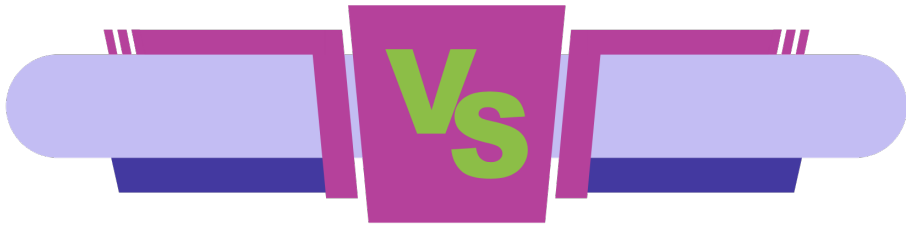
INSURED

- Timely issued coverage letter with a reservation of rights.
- Approve expenses and coverage within 30 days.
- Timely provide reimbursements.
- Document coverage decisions.
- Allow insured to select any panel vendor or reasonably approve non-panel vendors.
- Quickly respond to issues.

PLAYER ADVANTAGES

INSURER:

- More experienced – plays game constantly.
- More familiar with policy language and the “traps” therein.
- Knows the laws on coverage and policy interpretation.

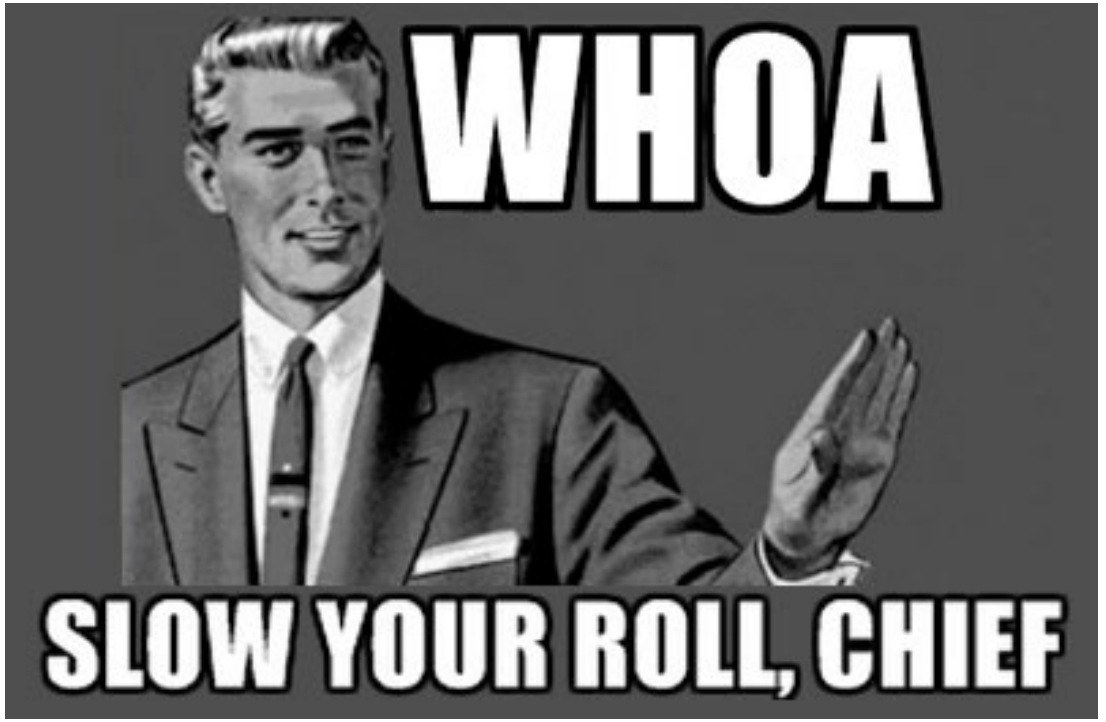


INSURED:

- Laws construed in favor of insured (all ambiguities used against insurer).
- Only required to convey certainties to the insurer – not your thoughts or speculation.
- Insurer “on the clock” for timely reimbursements and decisions. No such pressure on insured.
- Insureds only have to give insurer just enough information to trigger coverage.

REVEAL INFORMATION SLOWLY

- Force the insurer to ask questions, over-disclosure complicates coverage.
- Guessing information not confirmed through hard evidence (system logs, verifiable online posts) should **never** be conveyed to the insurer.
  - Insurers reserve the right to use any information for ***their benefit*** and lower coverage costs are in their best interests.
- The more you the adjuster, the more chances the adjuster will limit coverage.



SAMPLE CLAIM LETTER

The insurer will use any info given to them to deny coverage. Therefore, claim letters from insured should only include:

- The policy number.
- Effective date of the policy.
- The “on or about” date of the incident.
- A **basic** statement about the incident.
- A point of contact (and cc your attorney).

PANEL VENDORS

- Insurers want claims resolved AS QUICKLY AS POSSIBLE with PREDICTABLE COSTS.
  - *This is not always in insured's best interest.*
- Insurers use "panel" or "preferred" vendors, with pre-negotiated rates.
- Types of panel vendors:
  - Consumer monitoring services
  - Attorneys
  - Forensic services & network remediation
- **NOT ALL PANEL VENDORS ARE BAD!**
  - Many are amazing and leaders in research and development.
  - But, some insurers own panel vendors, negating free-market benefits.
    - Insurer essentially reimburse themselves through deductibles and setting rates.

PANEL VENDORS

beazley

To access **Post Breach Remedial Services**, the **Insured Organization** must:

1. notify the Underwriters that they desire to receive such services; and
2. enter into an engagement agreement with Lodestone to receive such services,

within sixty (60) days following a determination of the actual **Unauthorized Access or Use** of the **Insured Organization's Computer Systems**.

Beazley creates integrated cyber risk management company, Beazley Security

21st February 2024 - Author: Kane Wells

Specialty insurer Beazley has announced the merger of its in-house Cyber Services team with its wholly owned cyber security company Lodestone, creating an integrated cyber risk management company, Beazley Security.

VET VENDORS

- Google the vendor.
- Look at reviews.
- Ask attorney to check legal databases for lawsuits.
- Vendor owned by the insurer?
- Review vendor tools
  - "Beta" or "Open-source" software is a **RED FLAG**.
- Ensure forensics perform "memory malware analysis?"
  - **RED FLAG** if not.
  - Strict reliance on logging tools is insufficient for forensics.

```
| tstats `security_content_summariesonly` values(Processes.process) as process min(_time) as firstTime max(_tim
e) as lastTime from datamodel=Endpoint.Processes where Processes.process_name=wevtutil.exe Processes.process IN
("* cl *", "*clear-log*", "* -cl *") Processes.process IN ("*System*", "*Security*", "*Setup*", "*Application
*", "*trace*", "*powershell*") by Processes.parent_process_name Processes.parent_process Processes.process Proc
esses.process_guid Processes.process_id Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
|`security_content_ctime(lastTime)`
| `suspicious_wevtutil_usage_filter`
```

Wevtutil is a Windows tool for event log management that attackers exploit to erase & manipulate system logs, to malicious activity.

PANEL VENDORS

What is a breach counsel?
An attorney with ***some*** cybersecurity expertise, to assist Insured with navigating the cyber incident.

Who do breach counsel represent?
Officially, the Insured per an engagement agreement.

Who pays breach counsel?
The Insurer, after the deductible is met by Insured.

Who selects breach counsel?
The insurance company via panel vendor list with pre-negotiated rates. Insurers alert breach counsel to call insured after claim, unprompted by insured.

MAINTAIN OWN COUNSEL

- Breach counsel have temptation for conflicting loyalties.
  - Panel Vendors have guaranteed clientele.
- ***Not*** always proficient in technology and malware.
  - *Always looking for quickest band-aid, like paying ransom.*
- Encouraged to use other panel vendors, often without vetting.
- They have no history with the Insured, **meaning no motive to maintain that client relationship**.
- **ANSWER**: Hire own, local attorney who is involve in EVERY conversation you have with vendors.

HORROR STORY

***In Re Rutters Data Security Breach Litigation*, Case 1:20-cv-00382-JEJ-KM (M.D.Pa, 2021)**

A CAUTIONARY TALE…

- Discovery dispute for forensics report after PA convenience store data breach.
- Insurer assigns breach counsel, who hired a panel forensics vendor.
- Plaintiffs (victims of the breach) demanded forensics report (to support negligence claims).
- **Claim of legal privilege failed for 4 reasons**:
  - Forensic Vendor and Rutter often met privately;
  - Rutter (not Baker) paid Forensics Vendor directly;
  - Forensics Vendor provided its report directly to Rutter; and
  - The Forensic Vendor's contract did not include language about being prepared for litigation.
- Rutters **should have** used usual counsel (not breach) manage the claim and shield the black eyes.

APPLICATION

1. REVIEW YOUR POLICY TODAY – DOES IT MEET YOUR NEEDS?

2. ENSURE YOUR POLICY HAS ALL AVAILABLE FRAUD COVERAGE AND HIGH SOCIAL ENGINEERING COVERAGE LIMITS.

3. IMMEDIATELY CREATE A MFA POLICY (LIKE PHONE CALLS TO BANK TO CONFIRM ACCOUNT INFORMATION MATCHES PAYEE) FOR ELECTRONIC PAYMENTS.

4. DO NOT OVERSHARE WHEN SUBMITTING THE CLAIMS – CREATE A STANDARD CLAIM LETTER FOR FUTURE USE.

5. MAINTAIN YOUR OWN LEGAL COUNSEL, IF YOU DON'T HAVE A REGULAR, TRUSTED COUNSEL NOW, GET ONE!

Contact & Questions ~

Sarah Anderson

sarah@legallycyber.com

SWA LAW LLC

LEGALLYCYBER.COM

GREEN WALL

projectgreenwall.com

RSAC™ 2025 Conference

Many Voices.
One Community.

Sarah W. Anderson

(O) 225.256.2892 | Sarah@LegallyCyber.com

Licensed in LA, TX, PA, & IL